Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 25/03/2025 - 28/03/2025

Contents

Common Vulnerabilities and Exposures (CVEs)

URL ευπάθειας (NIST NVD)	CVSSv3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	Συσκευές/Εκδόσεις που ΔΕΝ επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2024-47516	**9,8**	An argument injection in Git	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	An argument injection in Git	n/a	https://access.redhat.com/security/cve/CVE-2024-47516 https://bugzilla.redhat.com/show_bug.cgi?id=2315805
https://nvd.nist.gov/vuln/detail/CVE-2024-42533	**9,8**	Convivance StandVoice	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'	4.5 through 6.2	n/a	https://gist.github.com/7h30th3r0n3/eae27e0eed39741365c55dfd46b57dc8 https://gist.github.com/7h30th3r0n3/eae27e0eed39741365c55dfd46b57dc8
https://nvd.nist.gov/vuln/detail/CVE-2025-2332	**9,8**	Export All Posts, Products, Orders, Refunds & Users plugin for WordPress	Deserialization of Untrusted Data	all versions up to, and including, 2.13	n/a	https://plugins.trac.wordpress.org/browser/wp-ultimate-exporter/trunk/exportExtensions/ExportExtension.php#L3332 https://plugins.trac.wordpress.org/changeset/3257504/ https://www.wordfence.com/threat-intel/vulnerabilities/id/9546ab46-737c-4bd3-9542-8ab1b776b3ea?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-2825	**9,8**	CrushFTP	Improper Authentication	versions 10.0.0 through 10.8.3 and 11.0.0 through 11.3.0	n/a	https://www.crushftp.com/crush11wiki/Wiki.jsp?page=Update https://www.rapid7.com/blog/post/2025/03/25/etr-notable-vulnerabilities-in-next-js-cve-2025-29927/ https://www.runzero.com/blog/crushftp/

https://nvd.nist.gov/vuln/detail/CVE-2025-28916	**9,8**	Docpro	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')	from n/a through 2.0.1	n/a	https://patchstack.com/database/wordpress/plugin/docpro/vulnerability/wordpress-docpro-plugin-2-0-1-local-file-inclusion-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-2294	**9,8**	The Kubio AI Page Builder	**Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')**	all versions up to, and including, 2.5.1	n/a	https://plugins.trac.wordpress.org/browser/kubio/tags/2.5.1/lib/integrations/third-party-themes/editor-hooks.php#L32 https://www.wordfence.com/threat-intel/vulnerabilities/id/2fb44c6e-520e-4a9f-9987-8b770feb710d?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-22398	**9,8**	Dell Unity	**Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')**	version(s) 5.4 and prior	n/a	https://www.dell.com/support/kbdoc/en-us/000300090/dsa-2025-116-security-update-for-dell-unity-dell-unityvsa-and-dell-unity-xt-security-update-for-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2025-26909	**9,6**	Hide My WP Ghost	**Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')**	from n/a through 5.4.01	n/a	https://patchstack.com/database/wordpress/plugin/hide-my-wp/vulnerability/wordpress-hide-my-wp-ghost-plugin-5-4-01-local-file-inclusion-to-rce-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-30216	**9,4**	the CCSDS Space Data Link Security Protocol - Extended Procedures (SDLS-EP)	Heap-based Buffer Overflow	versions 1.3.3 and prior	n/a	https://github.com/nasa/CryptoLib/commit/810fd66d592c883125272fef123c3240db2f170f https://github.com/nasa/CryptoLib/security/advisories/GHSA-v3jc-5j74-hcjv https://github.com/user-attachments/assets/d49cea04-ce84-4d60-bb3a-987e843f09c4
https://nvd.nist.gov/vuln/detail/CVE-2025-28904	**9,3**	Shamalli Web Directory Free	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Web Directory Free: from n/a through 1.7.6	n/a	https://patchstack.com/database/wordpress/plugin/web-directory-free/vulnerability/wordpress-web-directory-free-plugin-1-7-6-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-30524	**9,3**	Product Catalog	mproper Neutralization of Special Elements used	from n/a through 1.0.4	n/a	https://patchstack.com/database/wordpress/plugin/displayproduct/vulnerability/wordpress-

			in an SQL Command ('SQL Injection')			product-catalog-plugin-1-0-4-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-28942	**9,3**	Trust Payments Trust Payments Gateway for WooCommerce	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	n/a through 1.1.4	n/a	https://patchstack.com/database/wordpress/plugin/trust-payments-hosted-payment-pages-integration/vulnerability/wordpress-trust-payments-gateway-for-woocommerce-plugin-1-1-4-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-28898	**9,3**	WP Multistore Locator	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	from n/a through 2.5.2	n/a	https://patchstack.com/database/wordpress/plugin/wp-multi-store-locator/vulnerability/wordpress-wp-multistore-locator-plugin-2-5-2-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-26898	**9,3**	Traveler	**Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')**	from n/a through 3.1.8.	n/a	https://patchstack.com/database/wordpress/theme/traveler/vulnerability/wordpress-traveler-theme-3-1-8-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-24383	**9,1**	Dell Unity	**Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')**	version(s) 5.4 and prior	n/a	https://www.dell.com/support/kbdoc/en-us/000300090/dsa-2025-116-security-update-for-dell-unity-dell-unityvsa-and-dell-unity-xt-security-update-for-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2025-26873	**9**	Traveler	**Deserialization of Untrusted Data**	from n/a through 3.1.8.	n/a	https://patchstack.com/database/wordpress/theme/traveler/vulnerability/wordpress-traveler-theme-3-1-8-php-object-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-29635	**8,8**	D-Link	Improper Neutralization of Special Elements used in a Command ('Command Injection')	DIR-823X 240126 and 240802	n/a	https://github.com/mono7s/Dir-823x/blob/main/set_prohibiting/set_prohibiting.md

https://nvd.nist.gov/vuln/detail/CVE-2025-2319	**8,8**	EZ SQL Reports Shortcode Widget and DB Backup plugin for WordPress	Cross-Site Request Forgery (CSRF)	versions 4.11.13 to 5.25.08.	Version 5.25.10	https://plugins.trac.wordpress.org/browser/elisqlreports/tags/4..11.13/index.php https://plugins.trac.wordpress.org/browser/elisqlreports/tags/4..11.15/index.php https://plugins.trac.wordpress.org/browser/elisqlreports/tags/4..11.33/index.php https://plugins.trac.wordpress.org/browser/elisqlreports/tags/4.11.37/index.php https://plugins.trac.wordpress.org/browser/elisqlreports/tags/4.16.38/index.php https://plugins.trac.wordpress.org/browser/elisqlreports/tags/4.17.38/index.php https://plugins.trac.wordpress.org/browser/elisqlreports/tags/4.17.42/index.php https://plugins.trac.wordpress.org/browser/elisqlreports/tags/5.21.35/index.php https://plugins.trac.wordpress.org/browser/elisqlreports/tags/5.25.08/index.php https://www.wordfence.com/threat-intel/vulnerabilities/id/eade6ab0-ff79-4107-83ce-e85b37d97442?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-45352	**8,8**	Xiaomi smarthome	Origin Validation Error		n/a	https://trust.mi.com/zh-CN/misrc/bulletins/advisory?cveId=550
https://nvd.nist.gov/vuln/detail/CVE-2025-2837	**8,8**	Silicon Labs Gecko OS HTTP	Stack-based Buffer Overflow		n/a	https://community.silabs.com/a45Vm0000000Atp https://www.zerodayinitiative.com/advisories/ZDI-24-871/
https://nvd.nist.gov/vuln/detail/CVE-2025-2328	**8,8**	The Drag and Drop Multiple File Upload for Contact Form 7	**Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')**	all versions up to, and including, 1.3.8.7	n/a	https://plugins.trac.wordpress.org/browser/drag-and-drop-multiple-file-upload-contact-form-7/trunk/inc/dnd-upload-cf7.php#L153 https://plugins.trac.wordpress.org/changeset/3261964/ https://www.wordfence.com/threat-intel/vulnerabilities/id/0f6cca7a-b8ff-4ca5-b813-e611eac07695?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-24381	**8,8**	Dell Unity	**URL Redirection to Untrusted Site ('Open Redirect')**	version(s) 5.4 and prior	n/a	https://www.dell.com/support/kbdoc/en-us/000300090/dsa-2025-116-security-update-for-dell-unity-dell-unityvsa-and-dell-unity-xt-security-update-for-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2025-0811	**8,7**	GitLab CE/EE	**Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')**	all versions from 17.7 before 17.8.6, 17.9 before 17.9.3, and 17.10 before 17.10.1	n/a	https://gitlab.com/gitlab-org/gitlab/-/issues/515566 https://hackerone.com/reports/2961854
https://nvd.nist.gov/vuln/detail/CVE-2025-2255	**8,7**	Gitlab EE/CE	**Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')**	all versions from 13.5.0 before 17.8.6, 17.9 before 17.9.3, and 17.10 before 17.10.1	n/a	https://gitlab.com/gitlab-org/gitlab/-/issues/524635 https://hackerone.com/reports/2994150
https://nvd.nist.gov/vuln/detail/CVE-2024-13617	**8,6**	The aoa-downloadable WordPress plugin	CWE	0.1.0	n/a	https://wpscan.com/vulnerability/8d6dd979-21ef-4d14-9c42-bbd1d7b65c53/
https://nvd.nist.gov/vuln/detail/CVE-2025-30353	**8,6**	Directus	Exposure of Sensitive Information to an Unauthorized Actor	version 9.12.0 and prior to version 11.5.0	n/a	https://github.com/directus/directus/security/advisories/GHSA-fm3h-p9wm-h74h https://github.com/directus/directus/security/advisories/GHSA-fm3h-p9wm-h74h
https://nvd.nist.gov/vuln/detail/CVE-2025-28939	**8,5**	NotFound WP Google Calendar Manager	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	n/a through 2.1	n/a	https://patchstack.com/database/wordpress/plugin/wp-gcalendar/vulnerability/wordpress-wp-google-calendar-manager-plugin-2-1-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-22783	**8,5**	SEO Plugin by Squirrly SEO	**Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')**	from n/a through 12.4.03	n/a	https://patchstack.com/database/wordpress/plugin/squirrly-seo/vulnerability/wordpress-seo-plugin-by-squirrly-seo-plugin-12-4-03-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-2783	**8,3**	Mojo in Google Chrome on Windows	CWE	prior to 134.0.6998.177	n/a	https://chromereleases.googleblog.com/2025/03/stable-channel-update-for-desktop_25.html https://issues.chromium.org/issues/405143032

https://nvd.nist.gov/vuln/detail/CVE-2025-27147	**8,2**	The GLPI Inventory Plugin	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Versions prior to 1.5.0	Version 1.5.0	https://github.com/glpi-project/glpi-inventory-plugin/commit/aaeb26d98d07019375c25b56e60fffc195553545 https://github.com/glpi-project/glpi-inventory-plugin/security/advisories/GHSA-h6x9-jm98-cw7c
https://nvd.nist.gov/vuln/detail/CVE-2025-26733	**8,2**	Shinetheme Traveler	**Missing Authorization**	from n/a through 3.1.8	n/a	https://patchstack.com/database/wordpress/theme/traveler/vulnerability/wordpress-traveler-theme-3-1-8-broken-access-control-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-30232	**8,1**	Exim	**Use After Free**	4.96 through 4.98.1	n/a	http://www.openwall.com/lists/oss-security/2025/03/26/1 https://www.exim.org/static/doc/security/CVE-2025-30232.txt
https://nvd.nist.gov/vuln/detail/CVE-2025-30358	**8,1**	Mesop	**Improperly Controlled Modification of Dynamically-Determined Object**	prior to version 0.14.1	n/a	https://github.com/mesop-dev/mesop/commit/748e20d4a363d89b841d62213f5b0c6b4bed788f https://github.com/mesop-dev/mesop/security/advisories/GHSA-f3mf-hm6v-jfhh
https://nvd.nist.gov/vuln/detail/CVE-2025-20229	**8**	Splunk Enterprise	Improper Access Control	versions below 9.3.3, 9.2.5, and 9.1.8, and Splunk Cloud Platform versions below 9.3.2408.104, 9.2.2406.108, 9.2.2403.114, and 9.1.2312.208	n/a	https://advisory.splunk.com/advisories/SVD-2025-0301
https://nvd.nist.gov/vuln/detail/CVE-2025-2530	**7,8**	installations of Luxion KeyShot	Access of Uninitialized Pointer		n/a	https://www.zerodayinitiative.com/advisories/ZDI-25-173/
https://nvd.nist.gov/vuln/detail/CVE-2025-22230	**7,8**	VMware Tools for Windows	Authentication Bypass Using an Alternate Path or Channel		n/a	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25518

https://nvd.nist.gov/vuln/detail/CVE-2025-24386	**7,8**	Dell Unity	**Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')**	version(s) 5.4 and prior	n/a	https://www.dell.com/support/kbdoc/en-us/000300090/dsa-2025-116-security-update-for-dell-unity-dell-unityvsa-and-dell-unity-xt-security-update-for-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2025-24385	**7,8**	Dell Unity	**Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')**	version(s) 5.4 and prior	n/a	https://www.dell.com/support/kbdoc/en-us/000300090/dsa-2025-116-security-update-for-dell-unity-dell-unityvsa-and-dell-unity-xt-security-update-for-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2025-24379	**7,8**	Dell Unity	**Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')**	version(s) 5.4 and prior	n/a	https://www.dell.com/support/kbdoc/en-us/000300090/dsa-2025-116-security-update-for-dell-unity-dell-unityvsa-and-dell-unity-xt-security-update-for-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2025-24380	**7,8**	Dell Unity	**Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')**	version(s) 5.4 and prior	n/a	https://www.dell.com/support/kbdoc/en-us/000300090/dsa-2025-116-security-update-for-dell-unity-dell-unityvsa-and-dell-unity-xt-security-update-for-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2025-24381	**7,8**	Dell Unity	**Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')**	version(s) 5.4 and prior	n/a	https://www.dell.com/support/kbdoc/en-us/000300090/dsa-2025-116-security-update-for-dell-unity-dell-unityvsa-and-dell-unity-xt-security-update-for-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2025-24382	**7,8**	Dell Unity	**Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')**	version(s) 5.4 and prior	n/a	https://www.dell.com/support/kbdoc/en-us/000300090/dsa-2025-116-security-update-for-dell-unity-dell-unityvsa-and-dell-unity-xt-security-update-for-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2024-49565	**7,8**	Dell Unity	**Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')**	version(s) 5.4 and prior	n/a	https://www.dell.com/support/kbdoc/en-us/000300090/dsa-2025-116-security-update-for-dell-unity-dell-unityvsa-and-dell-unity-xt-security-update-for-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2024-49564	**7,8**	Dell Unity	**Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')**	version(s) 5.4 and prior	n/a	https://www.dell.com/support/kbdoc/en-us/000300090/dsa-2025-116-security-update-for-dell-unity-dell-unityvsa-and-dell-unity-xt-security-update-for-multiple-vulnerabilities

https://nvd.nist.gov/vuln/detail/CVE-2024-49563	**7,8**	Dell Unity	**Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')**	version(s) 5.4 and prior	n/a	https://www.dell.com/support/kbdoc/en-us/000300090/dsa-2025-116-security-update-for-dell-unity-dell-unityvsa-and-dell-unity-xt-security-update-for-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2025-27406	**7,6**	Icinga Reporting	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	versions 0.10.0 through 1.0.2	n/a	https://github.com/Icinga/icingaweb2-module-reporting/releases/tag/v1.0.3 https://github.com/Icinga/icingaweb2-module-reporting/security/advisories/GHSA-7qvq-54vm-r7hx
https://nvd.nist.gov/vuln/detail/CVE-2025-27405	**7,6**	Icinga Web 2	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	versions prior to 2.11.5 and 2.12.13	versions 2.11.5 and 2.12.3	https://github.com/Icinga/icingaweb2/releases/tag/v2.11.5 https://github.com/Icinga/icingaweb2/releases/tag/v2.12.3 https://github.com/Icinga/icingaweb2/security/advisories/GHSA-3x37-fjc3-ch8w
https://nvd.nist.gov/vuln/detail/CVE-2025-26956	**7,6**	Traveler	**Missing Authorization**	from n/a through 3.1.8.	n/a	https://patchstack.com/database/wordpress/theme/traveler/vulnerability/wordpress-traveler-theme-3-1-8-php-object-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-55073	**7,6**	/api/users/{user-id} of hay-kot mealie	**Missing Authorization**	v2.2.0	n/a	https://github.com/mealie-recipes/mealie/issues/4593 https://m10x.de/posts/2025/03/all-your-recipe-are-belong-to-us-part-3/3-broken-access-controls-leading-to-privilege-escalation-and-more-in-mealie/
https://nvd.nist.gov/vuln/detail/CVE-2025-22652	**7,6**	Payment Forms for Paystack	**Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')**	from n/a through 4.0.1	n/a	https://patchstack.com/database/wordpress/plugin/payment-forms-for-paystack/vulnerability/wordpress-payment-forms-for-paystack-plugin-4-0-1-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-30921	**7,6**	Newsletters	**Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')**	from n/a through 4.9.9.7	n/a	

https://nvd.nist.gov/vuln/detail/CVE-2025-30567	**7,5**	wp01ru WP01	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	WP01: from n/a through 2.6.2	n/a	https://patchstack.com/database/wordpress/plugin/wp01/vulnerability/wordpress-wp01-2-6-2-arbitrary-file-download-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-1445	**7,5**	RTU IEC 61850	Missing Synchronization		n/a	https://publisher.hitachienergy.com/preview?DocumentId=8DBD000207&languageCode=en&Preview=true
https://nvd.nist.gov/vuln/detail/CVE-2025-2485	**7,5**	The Drag and Drop Multiple File Upload for Contact Form 7	**Deserialization of Untrusted Data**	all versions up to, and including, 1.3.8.7	n/a	https://plugins.trac.wordpress.org/browser/drag-and-drop-multiple-file-upload-contact-form-7/trunk/inc/dnd-upload-cf7.php#L25 https://plugins.trac.wordpress.org/browser/drag-and-drop-multiple-file-upload-contact-form-7/trunk/inc/dnd-upload-cf7.php#L844 https://plugins.trac.wordpress.org/changeset/3261964/ https://www.wordfence.com/threat-intel/vulnerabilities/id/79ffe548-0005-4f5e-873f-a1afec64a251?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-26890	**7,5**	PluginUs.Net HUSKY	**Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')**	from n/a through 1.3.6.4	n/a	https://patchstack.com/database/wordpress/plugin/woocommerce-products-filter/vulnerability/wordpress-husky-plugin-1-3-6-4-local-file-inclusion-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-12905	**7,5**	tar-fs	**Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')**	from 0.0.0 before 1.16.4, from 2.0.0 before 2.1.2, from 3.0.0 before 3.0.8	n/a	https://github.com/mafintosh/tar-fs/commit/a1dd7e7c7f4b4a8bd2ab60f513baca573b44e2ed
https://nvd.nist.gov/vuln/detail/CVE-2025-2242	**7,5**	GitLab CE/EE	**Incorrect Authorization**	all versions from 17.4 prior to 17.8.6, 17.9 prior to 17.9.3, and 17.10 prior to 17.10.1	n/a	https://gitlab.com/gitlab-org/gitlab/-/issues/516271
https://nvd.nist.gov/vuln/detail/CVE-2024-58104	**7,3**	Trend Micro Apex One Security Agent	Improper Privilege Management	Trend Micro Apex One Security Agent	n/a	https://success.trendmicro.com/en-US/solution/KA-0018217

		Plug-in User Interface Manager		Plug-in User Interface Manager		
https://nvd.nist.gov/vuln/detail/CVE-2024-58105	**7,3**	Trend Micro Apex One Security Agent Plug-in User Interface Manager	Incorrect User Management	Trend Micro Apex One Security Agent Plug-in User Interface Manager	n/a	https://success.trendmicro.com/en-US/solution/KA-0018217
https://nvd.nist.gov/vuln/detail/CVE-2025-2740	**7,3**	PHPGurukul Old Age Home Management System	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	1.0	n/a	https://github.com/guimo3/cve/issues/1 https://github.com/guimo3/cve/issues/1 https://phpgurukul.com/ https://vuldb.com/?ctiid.300762 https://vuldb.com/?id.300762 https://vuldb.com/?submit.524733
https://nvd.nist.gov/vuln/detail/CVE-2025-2740	**7,3**	PHPGurukul Old Age Home Management System	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	1.0	n/a	https://github.com/guimo3/cve/issues/1 https://github.com/guimo3/cve/issues/1 https://phpgurukul.com/ https://vuldb.com/?ctiid.300762 https://vuldb.com/?id.300762 https://vuldb.com/?submit.524733
https://nvd.nist.gov/vuln/detail/CVE-2025-24383	**7,3**	Dell Unity	**Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')**	version(s) 5.4 and prior	n/a	https://www.dell.com/support/kbdoc/en-us/000300090/dsa-2025-116-security-update-for-dell-unity-dell-unityvsa-and-dell-unity-xt-security-update-for-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2025-24382	**7,3**	Dell Unity	**Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')**	version(s) 5.4 and prior	n/a	https://www.dell.com/support/kbdoc/en-us/000300090/dsa-2025-116-security-update-for-dell-unity-dell-unityvsa-and-dell-unity-xt-security-update-for-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2025-2846	**7,3**	SourceCodester Online Eyewear Shop	**Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')**	1.0	n/a	https://github.com/jeajeaa/cve/blob/main/sql.md https://vuldb.com/?ctiid.301492 https://vuldb.com/?id.301492 https://vuldb.com/?submit.522326 https://www.sourcecodester.com/

https://nvd.nist.gov/vuln/detail/CVE-2024-13690	**7,2**	The WP Church Donation plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	versions up to, and including, 1.7	n/a	http://plugins.svn.wordpress.org/wp-church-donation/tags/1.7/includes/church-donation-form-display.php http://plugins.svn.wordpress.org/wp-church-donation/tags/1.7/includes/church-donation-listings.php https://wordpress.org/plugins/wp-church-donation/ https://www.wordfence.com/threat-intel/vulnerabilities/id/de8ac20f-d6ae-4e55-9337-4fb5ebd4f24a?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-13618	**7,2**	aoa-downloadable WordPress plugin	CWE	0.1.0	n/a	https://wpscan.com/vulnerability/d6a78233-3f23-4da4-9bc0-1439cde20a30/
https://nvd.nist.gov/vuln/detail/CVE-2024-13863	**7,1**	The Stylish Google Sheet Reade	CWE	4.0 WordPress plugin before 4.1	n/a	https://wpscan.com/vulnerability/a6161595-0934-4baa-9da6-73792f4b87fd/
https://nvd.nist.gov/vuln/detail/CVE-2024-13863	**7,1**	The Stylish Google Sheet Reader	CWE	4.0 WordPress plugin before 4.1	n/a	https://wpscan.com/vulnerability/a6161595-0934-4baa-9da6-73792f4b87fd/
https://nvd.nist.gov/vuln/detail/CVE-2025-30355	**7,1**	Synapse	Improper Input Validation	version up to 1.127.0	v1.127.1	https://github.com/element-hq/synapse/commit/2277df2a1eb685f85040ef98fa21d41aa4cdd389 https://github.com/element-hq/synapse/releases/tag/v1.127.1 https://github.com/element-hq/synapse/security/advisories/GHSA-v56r-hwv5-mxg6
https://nvd.nist.gov/vuln/detail/CVE-2025-20231	**7,1**	Splunk Enterprise	Insertion of Sensitive Information into Log File	versions below 9.4.1, 9.3.3, 9.2.5, and 9.1.8, and versions below 3.8.38 and 3.7.23	n/a	https://advisory.splunk.com/advisories/SVD-2025-0302
https://nvd.nist.gov/vuln/detail/CVE-2025-28935	**7,1**	Fancybox Plus	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	n/a through 1.0.1	n/a	https://patchstack.com/database/wordpress/plugin/fancybox-plus/vulnerability/wordpress-fancybox-plus-plugin-1-0-1-reflected-cross-site-scripting-xss-vulnerability?_s_id=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-28934	**7,1**	Simple Post Series	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	from n/a through 2.4.4	n/a	https://patchstack.com/database/wordpress/plugin/simple-post-series/vulnerability/wordpress-simple-post-series-plugin-2-4-4-reflected-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-28928	**7,1**	Are you robot google recaptcha for word-press	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	from n/a through 2.2	n/a	https://patchstack.com/database/wordpress/plugin/are-you-robot-recaptcha/vulnerability/wordpress-are-you-robot-google-recaptcha-for-wordpress-plugin-2-2-reflected-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-28924	**7,1**	ZenphotoPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	from n/a through 1.8	n/a	https://patchstack.com/database/wordpress/plugin/zenphotopress/vulnerability/wordpress-zenphotopress-plugin-1-8-reflected-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-28921	**7,1**	SpatialMatch IDX	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	from n/a through 3.0.9	n/a	https://patchstack.com/database/wordpress/plugin/spatialmatch-free-lifestyle-search/vulnerability/wordpress-spatialmatch-idx-plugin-3-0-9-reflected-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-28917	**7,1**	Custom Smilies	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	from n/a through 2.9.2	n/a	https://patchstack.com/database/wordpress/plugin/custom-smilies-se/vulnerability/wordpress-custom-smilies-plugin-2-9-2-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-28911	**7,1**	Gravity 2 PDF	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	from n/a through 3.1.3	n/a	https://patchstack.com/database/wordpress/plugin/gf2pdf/vulnerability/wordpress-gravity-2-pdf-plugin-3-1-3-reflected-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-28903	**7,1**	Driving Directions	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	from n/a through 1.4.4	n/a	https://patchstack.com/database/wordpress/plugin/ddirections/vulnerability/wordpress-driving-directions-plugin-1-4-4-reflected-cross-site-scripting-xss-vulnerability?_s_id=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-28899	**7,1**	WP Event Ticketing	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	from n/a through 1.3.4	n/a	https://patchstack.com/database/wordpress/plugin/wpeventticketing/vulnerability/wordpress-wp-event-ticketing-plugin-1-3-4-reflected-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-28890	**7,1**	Lightview Plus	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	from n/a through 3.1.3	n/a	https://patchstack.com/database/wordpress/plugin/lightview-plus/vulnerability/wordpress-lightview-plus-plugin-3-1-3-reflected-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-28889	**7,1**	Custom Product Stickers for Woocommerce	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	from n/a through 1.9.0	n/a	https://patchstack.com/database/wordpress/plugin/custom-product-stickers-for-woocommerce/vulnerability/wordpress-custom-product-stickers-for-woocommerce-plugin-1-9-0-reflected-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-28889	**7,1**	Custom Product Stickers for Woocommerce		from n/a through 1.9.0	n/a	https://patchstack.com/database/wordpress/plugin/custom-product-stickers-for-woocommerce/vulnerability/wordpress-custom-product-stickers-for-woocommerce-plugin-1-9-0-reflected-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-26874	**7,1**	MemberSpace	**Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')**	from n/a through 2.1.13	n/a	https://patchstack.com/database/wordpress/plugin/memberspace/vulnerability/wordpress-memberspace-plugin-2-1-13-reflected-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-22628	**7,1**	Filled In	**Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')**	from n/a through 1.9.2	n/a	https://patchstack.com/database/wordpress/plugin/filled-in/vulnerability/wordpress-filled-in-plugin-1-9-1-csrf-to-stored-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-22658	**7,1**	Listings for Appfolio	**Cross-Site Request Forgery (CSRF)**	from n/a through 1.2.0	n/a	https://patchstack.com/database/wordpress/plugin/listings-for-appfolio/vulnerability/wordpress-listings-for-appfolio-plugin-1-2-0-csrf-to-stored-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-25100	**7,1**	Cazamba	**Cross-Site Request Forgery (CSRF)**	from n/a through 1.2	n/a	https://patchstack.com/database/wordpress/plugin/cazamba/vulnerability/wordpress-

						cazamba-plugin-1-2-csrf-to-reflected-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-25086	**7,1**	Secret Meta	**Cross-Site Request Forgery (CSRF)**	from n/a through 1.2.1	n/a	https://patchstack.com/database/wordpress/plugin/facebook-secret-meta/vulnerability/wordpress-secret-meta-plugin-1-2-1-csrf-to-reflected-cross-site-scripting-xss-vulnerability?_s_id=cve

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Releases One Industrial Control Systems Advisory	▪ ICSA-25-037-01 Schneider Electric EcoStruxure Power Monitoring Expert (PME) (Update A)	https://www.cisa.gov/news-events/alerts/2025/03/27/cisa-releases-one-industrial-control-systems-advisory
CISA Adds One Known Exploited Vulnerability to Catalog	CVE-2025-2783	https://www.cisa.gov/news-events/alerts/2025/03/27/cisa-adds-one-known-exploited-vulnerability-catalog
CISA Adds Two Known Exploited Vulnerabilities to Catalog	CVE-2019-9874, CVE-2019-9875	https://www.cisa.gov/news-events/alerts/2025/03/26/cisa-adds-two-known-exploited-vulnerabilities-catalog
CISA Releases Four Industrial Control Systems Advisories	▪ ICSA-25-084-01 ABB RMC-100 ▪ ICSA-25-084-02 Rockwell Automation Verve Asset Manager ▪ ICSA-25-084-03 Rockwell Automation 440G TLS-Z ▪ ICSA-25-084-04 Inaba Denki Sangyo CHOCO TEI WATCHER Mini	https://www.cisa.gov/news-events/alerts/2025/03/25/cisa-releases-four-industrial-control-systems-advisories
CISA Adds One Known Exploited Vulnerability to Catalog	CVE-2025-30154	https://www.cisa.gov/news-events/alerts/2025/03/24/cisa-adds-one-known-exploited-vulnerability-catalog
Critical Vulnerabilities in Kubernetes Ingress-NGINX	CVE-2025-1097, CVE-2025-1098, CVE-2025-24514, CVE-2025-1974	https://cow-prod-www-v3.azurewebsites.net/publications/security-advisories/2025-012/

News

Σύντομη περιγραφή / Τίτλος	URL
Top 3 MS Office Exploits Hackers Use in 2025 – Stay Alert!	https://thehackernews.com/2025/03/top-3-ms-office-exploits-hackers-use-in.html
Fake Snow White Movie Torrent Infects Devices with Malware	https://hackread.com/fake-snow-white-movie-torrent-infects-device-malware/
Cloud Attacks Raises by Five Times Attacking Sensitive IAM Service Accounts	https://cybersecuritynews.com/cloud-attacks-raises-by-five-times/
The 4 WordPress flaws hackers targeted the most in Q1 2025	https://www.bleepingcomputer.com/news/security/the-four-wordpress-flaws-hackers-targeted-the-most-in-q1-2025/
Cloudflare R2 Service Outage: A Case Study in Human Error and System Design	https://dailysecurityreview.com/security-spotlight/cloudflare-r2-service-outage-a-case-study-in-human-error-and-system-design/
U.S. CISA adds Sitecore CMS and XP, and GitHub Action flaws to its Known Exploited Vulnerabilities catalog	https://securityaffairs.com/175915/security/u-s-cisa-adds-sitecore-cms-and-xp-and-github-action-flaws-to-its-known-exploited-vulnerabilities-catalog.html
Lengthy disruption of Russian internet provider claimed by Ukrainian hacker group	https://therecord.media/russia-isp-lovit-outages-claimed-ukraine-it-army?&web_view=true
Arkana Security group claims the hack of US telco provider WideOpenWest (WOW!)	https://securityaffairs.com/175905/data-breach/arkana-security-group-claims-the-hack-of-wideopenwest-wow.html
NIST Still Struggling to Clear Vulnerability Submissions Backlog in NVD	https://www.securityweek.com/nist-still-struggling-to-clear-vulnerability-submissions-backlog-in-nvd/
Fake DeepSeek Ads Spread Malware to Google Users	https://www.darkreading.com/vulnerabilities-threats/fake-deepseek-ads-spread-malware-google
Meet the Low-Key Access Broker Supercharging Russian State Cybercrime	https://www.darkreading.com/cyberattacks-data-breaches/access-broker-russian-state-cybercrime

Oracle Denies Claim of Oracle Cloud Breach of 6M Records	https://www.darkreading.com/cyberattacks-data-breaches/oracle-denies-claim-oracle-cloud-breach-6m-records
FBI Warns of Document Converter Tools Due to Uptick in Scams	https://www.darkreading.com/cyberattacks-data-breaches/fbi-document-converter-tools-scam

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Chinese Hackers Breach Asian Telecom, Remain Undetected for Over 4 Years	https://thehackernews.com/2025/03/chinese-hackers-breach-asian-telecom.html
NSW Government Website Data Breach With 9,000 Court files	https://dailysecurityreview.com/security-spotlight/nsw-government-website-data-breach-with-9000-court-files/
Numotion Data Breach Impacts Nearly 500,000 Individuals	https://dailysecurityreview.com/security-spotlight/numotion-data-breach-impacts-nearly-500000-individuals/
Arkana Ransomware Group Claims Compromise of US Telecom Companies	https://cybersecuritynews.com/arkana-ransomware-group-claims-compromise/
South Carolina Eye Clinic Suffers Data Breach: Ransomware Suspected	https://dailysecurityreview.com/security-spotlight/south-carolina-eye-clinic-suffers-data-breach-ransomware-suspected/
UK fines software provider £3.07 million for 2022 ransomware breach	https://www.bleepingcomputer.com/news/security/uk-fines-software-provider-307-million-for-2022-ransomware-breach/
Sydney Tools Data Breach Exposes 34 Million+ Customer Orders	https://dailysecurityreview.com/security-spotlight/sydney-tools-data-breach-exposes-34-million-customer-orders/
Cyberattack hits Ukrainian state railway, disrupting online ticket sales	https://therecord.media/ukraine-railway-ukrzaliznytsia-cyberattack-online-ticket-system?&web_view=true
Hijacked Microsoft Stream classic domain "spams" SharePoint sites	https://www.bleepingcomputer.com/news/microsoft/hijacked-microsoft-stream-classic-domain-spams-sharepoint-sites

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
CISA Warns of Sitecore RCE Flaws; Active Exploits Hit Next.js and DrayTek Devices	https://thehackernews.com/2025/03/cisa-flags-two-six-year-old-sitecore.html
New Security Flaws Found in VMware Tools and CrushFTP — High Risk, No Workaround	https://thehackernews.com/2025/03/new-security-flaws-found-in-vmware.html
EncryptHub Exploits Windows Zero-Day to Deploy Rhadamanthys and StealC Malware	https://thehackernews.com/2025/03/encrypthub-exploits-windows-zero-day-to.html
New Sophisticated Linux-Backdoor Attacking OT Systems Exploiting 0-Day RCE	https://cybersecuritynews.com/new-sophisticated-linux-backdoor-attacking-ot-systems/
Critical Next.js Vulnerability Allows Attackers to Bypass Middleware Authorization Checks	https://thehackernews.com/2025/03/critical-nextjs-vulnerability-allows.html
New SparrowDoor Backdoor Variants Found in Attacks on U.S. and Mexican Organizations	https://thehackernews.com/2025/03/new-sparrowdoor-backdoor-variants-found.html
U.S. CISA adds Google Chromium Mojo flaw to its Known Exploited Vulnerabilities catalog	https://securityaffairs.com/175936/security/u-s-cisa-adds-google-chromium-mojo-flaw-to-its-known-exploited-vulnerabilities-catalog.html

Mozilla warns Windows users of critical Firefox sandbox escape flaw	https://www.bleepingcomputer.com/news/security/mozilla-warns-windows-users-of-critical-firefox-sandbox-escape-flaw/
Russian Ransomware Gang Exploited Windows Zero-Day Before Patch	https://www.securityweek.com/russian-ransomware-gang-exploited-windows-zero-day-before-patch/
Dozens of solar inverter flaws could be exploited to attack power grids	https://www.bleepingcomputer.com/news/security/dozens-of-solar-inverter-flaws-could-be-exploited-to-attack-power-grids/
CrushFTP: Patch critical vulnerability ASAP! (CVE-2025-2825)	https://www.helpnetsecurity.com/2025/03/27/crushftp-vulnerability-cve-2025-2825/
Next.js Middleware Flaw Lets Attackers Bypass Authorization	https://hackread.com/next-js-middleware-flaw-bypass-authorization/
Zero-Day Alert: Google Releases Chrome Patch for Exploit Used in Russian Espionage Attacks	https://thehackernews.com/2025/03/zero-day-alert-google-releases-chrome.html

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Mozilla Patches Critical Firefox Bug Similar to Chrome's Recent Zero-Day Vulnerability	https://thehackernews.com/2025/03/mozilla-patches-critical-firefox-bug.html
Windows 11 KB5053656 update released with 38 changes and fixes	https://www.bleepingcomputer.com/news/microsoft/windows-11-kb5053656-update-released-with-38-changes-and-fixes/
Tor Browser 14.0.8 Released Emergency Update for Windows Users	https://cybersecuritynews.com/tor-browser-14-0-8-released-emergency-update/
Windows 11 24H2 Update Breaks Connection to the Veeam Backup Server	https://cybersecuritynews.com/windows-11-24h2-update-breaks-veeam/
Dangerous npm package ‘patches’ legitimate software with malware	https://scmagazine.com/news/dangerous-npm-package-patches-legitimate-software-with-malware
Zero-Day Alert: Google Releases Chrome Patch for Exploit Used in Russian Espionage Attacks	https://thehackernews.com/2025/03/zero-day-alert-google-releases-chrome.html
Splunk Patches Dozens of Vulnerabilities	https://www.securityweek.com/splunk-patches-dozens-of-vulnerabilities/
Urgent Security Update: Authentication Bypass Vulnerability in VMware Tools for Windows (CVE-2025-22230)	https://dailysecurityreview.com/security-spotlight/urgent-security-update-authentication-bypass-vulnerability-in-vmware-tools-for-windows-cve-2025-22230/

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
RedCurl Cyberespionage Group Deploys Ransomware Targeting Hyper-V	https://dailysecurityreview.com/security-spotlight/redcurl-cyberespionage-group-deploys-ransomware-targeting-hyper-v/
GorillaBot Attacks Windows Devices With 300,000+ Attack Commands Across 100+ Countries	https://cybersecuritynews.com/gorillabot-attacks-windows/

Threat Actors Using Powerful Cybercriminal Weapon 'Atlantis AIO' to Automate Credential Stuffing Attacks	**https://cybersecuritynews.com/threat-actors-using-powerful-cybercriminal-weapon-atlantis-aio/**
Crooks target DeepSeek users with fake sponsored Google ads to deliver malware	**https://securityaffairs.com/175923/malware/crooks-deepseek-users-with-fake-sponsored-google-ads-to-deliver-malware.html**
EncryptHub Exploits Windows Zero-Day to Deploy Rhadamanthys and StealC Malware	**https://thehackernews.com/2025/03/encrypthub-exploits-windows-zero-day-to.html**
Pakistan APT Hackers Create Weaponized IndiaPost Website to Attack Windows & Android Users	**https://cybersecuritynews.com/pakistan-apt-hackers-create-weaponized-indiapost-website/**
CISA Warns of Sitecore RCE Flaws; Active Exploits Hit Next.js and DrayTek Devices	**https://thehackernews.com/2025/03/cisa-flags-two-six-year-old-sitecore.html**

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Top 10 Best Cyber Attack Simulation Tools – 2025	**https://cybersecuritynews.com/cyber-attack-simulation-tools/**
Top Cybersecurity Tools of 2025 To Managing Remote Device Threats	**https://cybersecuritynews.com/top-cybersecurity-tools-managing-remote-device-threats/**

References

[1]. Ο βαθμός επικινδυνότητας είναι σύμφωνα με την κλίμακα Common Vulnerability Scoring System (CVSSv3), https://nvd.nist.gov/vuln-metrics/cvss

[2]. Τα CVEs αποτελέσματα που εμφανίζονται στην ενότητα 1 διαθέτουν CVSSv3 score >= 7.0 και έχει γίνει μια επιλογή συστημάτων/υπηρεσιών ανάλογα με το πόσο διαδεδομένα είναι.

[3]. Τα CVEs που αφορούν Wordpress plugins θα εμφανίζονται σε ξεχωριστή ενότητα (1.1) σε περιόδους που η εμφάνισή τους είναι ιδιαίτερα αυξημένη.

Annex – Websites with vendor specific vulnerabilities

Ο πίνακας περιέχει websites από κατασκευαστές που προσφέρουν πληροφορίες σχετικές με ευπάθειες που εμφανίζονται στα προϊόντα τους.

Vendor name / Platform	URL
Wordpress	Wordfence Intelligence Vulnerability Database API https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/ Scan your WordPress website, https://wpscan.com/scan/
Oracle	Critical Patch Updates, Security Alerts and Bulletins, https://www.oracle.com/security-alerts/
Fortinet	Fortinet products, https://www.fortiguard.com/psirt
IBM	Security bulletins, https://cloud.ibm.com/status/security Research, Collaborate and Act on threat intelligence, https://exchange.xforce.ibmcloud.com/
MS Windows	The Microsoft Security Response Center (MSRC), https://msrc.microsoft.com/update-guide/
SAP	SAP Security Notes, https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html
Dell	Security Advisories, Notices and Resources, https://www.dell.com/support/security/en-us
HPE	HPE Security Bulletin Library, https://support.hpe.com/connect/s/securitybulletinlibrary Security Bulletins, https://support.hp.com/us-en/security-bulletins
Cisco	Cisco Security Advisories, https://sec.cloudapps.cisco.com/security/center/publicationListing.x
Palo Alto	Palo Alto Networks Security Advisories, https://security.paloaltonetworks.com/
Ivanti	Security Advisory, https://www.ivanti.com/blog/topics/security-advisory
Mozilla	Mozilla Foundation Security Advisories, https://www.mozilla.org/en-US/security/advisories/
Android	Android Security Bulletins, https://source.android.com/docs/security/bulletin/asb-overview
Zyxel	Security Advisories, https://www.zyxel.com/global/en/support/security-advisories
D-Link	Global Security Advisories, Responses, and Notices, https://supportannouncement.us.dlink.com/
Adobe	Security Bulletins and Advisories, https://helpx.adobe.com/security/security-bulletin.html
Siemens	Siemens ProductCERT and Siemens CERT, https://www.siemens.com/global/en/products/services/cert.html
Splunk	Splunk Security Advisories, https://advisory.splunk.com/